International Journal of Engineering Research and Science & Technology

www.ijerst.org

ISSN : 2319-5991

Vol. 18 No. 4 (2022)

ijerst.editor@gmail.com

editor@ijerst.com

International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 18, No. 4, 2022
© 2022 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Research Paper

BLOCKCHAIN-BASED SECURITY FRAMEWORK FOR PROTECTING DISTRIBUTED INDUSTRIAL IOT COMMUNICATION NETWORKS

Prof. Ming Chen
Research scholar

ABSTRACT

The rapid expansion of Industrial Internet of Things technologies has transformed modern manufacturing, energy, transportation, process automation, and cyber-physical production environments by enabling continuous communication among sensors, machines, programmable controllers, edge devices, gateways, cloud platforms, and enterprise applications. Although distributed Industrial IoT communication improves operational visibility, automation, predictive maintenance, and real-time decision-making, it also creates significant cybersecurity risks because heterogeneous devices exchange sensitive operational information across geographically distributed and potentially untrusted network environments. Conventional centralized security architectures frequently suffer from single points of failure, limited transaction traceability, weak device trust management, fragmented authentication, insecure application programming interfaces, and vulnerability to communication manipulation. This paper proposes a blockchain-based security framework for protecting distributed Industrial IoT communication networks. The framework integrates permissioned blockchain infrastructure, decentralized device identity management, cryptographically protected communication records, smart contract-based access control, secure API lifecycle management, edge-assisted validation, distributed event auditing, anomaly-aware transaction monitoring, and adaptive security policy enforcement. Industrial devices are registered through controlled identity procedures and their communication requests are evaluated according to authenticated identities, assigned roles, operational context, and predefined security policies. Security-relevant communication events are recorded through tamper-resistant distributed records, enabling traceability across heterogeneous industrial domains. The methodology also incorporates traffic integrity verification to reduce risks associated with man-in-the-middle manipulation, unauthorized message modification, replay attempts, compromised intermediaries, and coercive transaction behavior. Edge gateways reduce blockchain processing overhead by aggregating validated events and separating time-critical machine communication from noncritical audit operations. Representative experimental evaluation demonstrates that the proposed framework improves unauthorized access detection, communication integrity, auditability, and resilience against distributed attacks while maintaining acceptable latency for industrial monitoring applications. Comparative analysis indicates improved security effectiveness over centralized authentication and conventional access-control architectures. The proposed framework provides a scalable foundation for trustworthy, resilient, interoperable, and security-aware Industrial IoT ecosystems.

Keywords: Blockchain, Industrial Internet of Things, IIoT Security, Distributed Networks, Smart Contracts, Cybersecurity, Device Authentication, Secure Communication, Edge Computing, Industry 4.0.

I. INTRODUCTION

The Industrial Internet of Things (IIoT) has become a fundamental technology for Industry 4.0 by enabling intelligent communication among sensors, controllers, machines, edge devices, cloud platforms, and enterprise applications. Continuous connectivity improves manufacturing automation, predictive maintenance, process monitoring, and operational decision-making. However, the growing number of interconnected industrial devices also increases cybersecurity risks, making secure communication and trusted data exchange essential requirements for modern industrial environments [1], [2].

Blockchain technology has emerged as a promising solution for securing distributed Industrial IoT networks by providing decentralized trust, immutable transaction records, transparent auditing, and tamper-resistant data management. Unlike conventional centralized security mechanisms, blockchain reduces dependency on a single trusted authority while improving traceability and integrity of industrial communication. These characteristics make blockchain particularly suitable for protecting critical industrial infrastructures operating across distributed environments [3], [4].

Smart contracts further enhance blockchain-based security by enabling automated authorization, decentralized access control, and policy enforcement among industrial devices and applications. At the same time, standardized API architectures facilitate secure communication between IIoT gateways, cloud services, Digital Twins, and enterprise systems, ensuring interoperability across heterogeneous industrial platforms while supporting secure service integration [5], [6].

Modern Industrial IoT systems also require secure API lifecycle management to protect sensitive credentials, service interfaces, and communication channels throughout deployment and operation. Integrating blockchain with secure API management provides stronger authentication, improved access governance, and enhanced protection against unauthorized interactions within distributed industrial ecosystems [7], [8].

Despite significant advancements in Industrial IoT security, many existing solutions still face challenges related to centralized trust management, communication integrity, scalability, and secure service interoperability. Therefore, this research proposes a blockchain-based security framework that integrates decentralized trust, smart contracts, secure API lifecycle management, Digital Twin support, and Industrial IoT communication protection to improve cybersecurity, operational reliability, and trusted information exchange across distributed industrial networks [9], [10].

II. LITERATURE SURVEY

Kumar (2012) proposed a predictive maintenance framework based on IoT sensor data fusion for industrial machinery. The study demonstrated that integrating multiple sensor observations improves machinery health assessment, fault diagnosis, and predictive maintenance accuracy. The research also emphasized the importance of trustworthy industrial data for intelligent decision-making within connected manufacturing environments [11].

Narapareddy and Yerramilli (2021) presented a sustainable IT operation framework focusing on efficient infrastructure management, resource optimization, and secure enterprise computing practices. Their work highlighted the importance of reliable operational governance and sustainable software infrastructure for supporting modern distributed industrial systems [12].

Atlam et al. (2018) reviewed the state-of-the-art developments, applications, and security challenges of the Internet of Things. The authors identified authentication, privacy preservation,

device heterogeneity, secure communication, and scalable management as major research challenges requiring robust security architectures for Industrial IoT deployments [13].

Pokala (2022) proposed a practical MLOps framework for healthcare claims processing using production machine learning and automated model governance. Although developed for healthcare systems, the framework demonstrated the importance of secure deployment, model lifecycle management, scalable cloud-native architectures, and continuous operational monitoring, which are also applicable to Industrial IoT security platforms [14].

Restuccia, D'Oro, and Melodia (2018) investigated the integration of machine learning and software-defined networking for securing Internet of Things environments. Their study demonstrated that intelligent threat detection and adaptive network management significantly improve protection against evolving cyberattacks targeting distributed IoT infrastructures [15].

Kumar (2014) introduced a Digital Twin-based smart manufacturing framework for real-time process optimization by integrating virtual models with physical industrial assets. The study demonstrated that continuous synchronization between physical equipment and Digital Twins improves manufacturing visibility, operational monitoring, and intelligent industrial decision-making [16].

Conti et al. (2018) reviewed Internet of Things security and digital forensics, identifying major challenges related to cyberattacks, evidence collection, privacy protection, and secure incident investigation. Their work emphasized the necessity of trustworthy communication and traceable security mechanisms within distributed IoT infrastructures [17].

Lu, Xu, and Wang (2019) reviewed smart manufacturing process automation and discussed the integration of cloud computing, Industrial IoT, Digital Twins, and intelligent analytics. The authors concluded that intelligent cloud-enabled manufacturing platforms significantly improve operational efficiency, predictive maintenance, and industrial automation while requiring secure communication infrastructures [18].

Ferrag et al. (2018) surveyed authentication and privacy-preserving mechanisms for modern communication networks and demonstrated that robust authentication protocols, secure identity management, and privacy-aware communication significantly strengthen distributed network security against advanced cyber threats. Their findings provide valuable guidance for securing Industrial IoT communication environments [19].

Gummadi (2020) discussed API design and implementation using RAML and OpenAPI specifications for enterprise software integration. The study emphasized that standardized API specifications improve interoperability, maintainability, authentication, and secure communication among distributed services. These principles are highly relevant for blockchain-enabled Industrial IoT systems requiring secure interaction among sensors, gateways, cloud platforms, Digital Twins, and enterprise applications [20].

III. PROPOSED METHODOLOGY

The proposed methodology develops a blockchain-based security framework specifically designed for distributed Industrial IoT communication networks. The framework recognizes that industrial communication environments contain heterogeneous devices with different computational capabilities, operational responsibilities, network protocols, and security requirements. Rather than forcing every sensor message directly through a blockchain network, the methodology employs a layered architecture in which time-critical physical communication remains responsive while security-relevant identities, authorization

events, integrity evidence, policy changes, and significant transactions are validated through a permissioned blockchain infrastructure.

The physical industrial layer contains sensors, actuators, CNC machines, robotic systems, programmable logic controllers, industrial motors, manufacturing cells, energy systems, process equipment, Digital Twin-connected assets, and other cyber-physical resources. Each participating entity is assigned a controlled digital identity during registration. The identity record associates the device with its approved owner, equipment class, operational role, network domain, permitted services, and security status. This process reduces dependence on unauthenticated device addresses that may be spoofed or reassigned.

The device onboarding process begins with administrative or automated verification of the industrial asset. A device is accepted only after its identity information and deployment context have been validated according to organizational policy. Approved devices receive cryptographic credentials and a corresponding blockchain identity reference. Sensitive private credentials are not exposed directly within distributed records. Instead, the blockchain stores appropriate identity evidence, registration status, public verification information, and lifecycle events required for distributed trust decisions.

The permissioned blockchain layer is selected because industrial organizations generally require controlled participation rather than unrestricted anonymous consensus. Authorized industrial sites, security servers, edge domains, or organizational units operate validating nodes. Membership policies determine which entities may submit transactions, validate records, inspect specific information, or modify smart contract configurations. This controlled architecture provides stronger governance and lower processing overhead than unrestricted public blockchain networks.

The communication security process evaluates every important interaction according to source identity, destination identity, requested operation, device role, current security status, and applicable policy. Routine sensor transmission can continue through optimized industrial channels after authentication, while security-relevant evidence is submitted to the blockchain audit process. This selective strategy prevents the distributed ledger from becoming overloaded by high-frequency raw sensor streams.

Smart contracts implement consistent security policies across participating network domains. Policies define which device classes may communicate with specific services, which gateways may forward critical data, which applications may access machine information, and which administrative roles may modify security configurations. When an authorization request is received, the relevant policy logic evaluates the authenticated identity and requested operation. The result is recorded when the interaction has security significance.

Role-based and attribute-aware access principles are combined within the methodology. A maintenance application may receive access to equipment health data but not production control functions. A Digital Twin synchronization service may update approved virtual state attributes but may not modify device identities. An external analytics service may receive filtered information while being prevented from accessing sensitive control messages. This separation limits the consequences of compromised accounts and reduces excessive privileges.

The framework incorporates communication integrity verification to protect against unauthorized message modification. Security-sensitive messages contain verification evidence that allows receiving services to determine whether content has changed during transmission. Important communication events

are associated with trusted timestamps, device identities, and transaction references. This process strengthens traceability when information passes through multiple gateways or network domains.

Protection against man-in-the-middle behavior is addressed through authenticated communication relationships and verification of expected endpoints. The framework does not assume that an intermediary is trustworthy merely because it is located within the industrial network. Gateways and service endpoints must establish validated identities before sensitive information exchange. Unexpected changes in communication path, identity relationships, transaction behavior, or endpoint characteristics are treated as suspicious events.

The security design incorporates principles relevant to the traffic manipulation threats examined by Maturi. Distributed communication systems can be exposed to redirection, coercion, intermediary manipulation, and unauthorized alteration of protocol behavior. Within the proposed IIoT environment, the framework maintains trusted records of device relationships, detects unusual communication changes, and records significant integrity failures. This approach provides evidence for investigating attempts to manipulate industrial information flows.

Replay protection is incorporated because attackers may capture legitimate industrial messages and retransmit them later. Security-sensitive communication events contain freshness information and transaction context. Repeated or temporally inconsistent requests are rejected or escalated for investigation. The framework maintains recent event knowledge at edge gateways so that obvious replay attempts can be detected without waiting for remote blockchain validation.

The edge security layer plays a central role in maintaining industrial responsiveness. Edge gateways authenticate local devices, validate message structure, apply preliminary access rules, identify obvious anomalies, and aggregate security-relevant events. Only selected events are forwarded for distributed ledger recording. This architecture significantly reduces transaction volume and prevents high-frequency machine data from overwhelming blockchain validators.

Edge gateways are themselves treated as controlled security entities. Each gateway possesses a registered identity and limited permissions. A gateway may validate devices within its assigned industrial zone but cannot automatically modify policies for another zone. If a gateway behaves abnormally, its security status can be updated and distributed across the permissioned network. Other participants can then restrict or reject interactions originating from the compromised domain.

The API security layer protects interactions among IIoT platforms, Digital Twins, cloud analytics, maintenance applications, enterprise services, and blockchain components. Structured API specifications improve interface consistency, reflecting the design principles discussed by Gummadi. Each service interaction is authenticated and evaluated according to approved permissions. API endpoints are classified according to sensitivity so that machine monitoring requests, administrative operations, and control-related interactions receive different protection levels.

Secure API lifecycle management is incorporated from design through retirement. Development interfaces, testing credentials, production secrets, access tokens, and integration keys are governed according to controlled procedures. The methodology reflects the security principles emphasized by Gummadi regarding secrets protection. Blockchain records provide distributed evidence of significant authorization and policy events, while dedicated secrets management mechanisms protect sensitive credentials. This separation avoids the

insecure practice of placing confidential secrets directly on an immutable ledger.

The proposed framework also supports predictive maintenance systems. The sensor fusion principles discussed by Kumar demonstrate that industrial machinery monitoring depends on information from multiple sensing sources. Within the proposed architecture, sensor data used for maintenance analytics are associated with trusted device identities and communication provenance. Security-relevant metadata allow analytical services to determine whether information originated from approved sources and whether significant integrity anomalies occurred during transmission.

Digital Twin environments are similarly protected. Kumar's work on Digital Twin-based smart manufacturing demonstrates the importance of continuous physical-to-virtual information exchange. The proposed framework authenticates devices and services participating in Digital Twin synchronization. Significant virtual state updates can be associated with trusted provenance evidence, reducing the risk that compromised or unauthorized sources silently modify critical virtual representations.

Manufacturing process information is protected according to operational importance. The machining parameter optimization research of Kumar demonstrates that process settings influence tool wear and surface quality. Unauthorized manipulation of these settings may therefore affect both equipment condition and production outcomes. The framework records security-sensitive parameter modification events and verifies whether the requesting identity possesses appropriate authorization.

The methodology also considers metal additive manufacturing processes. Kumar's research on optimization of process parameters in metal additive manufacturing using machine learning demonstrates the importance of reliable process information for defect reduction. In distributed IIoT environments, machine learning models depend on trustworthy sensor and parameter data. The proposed security framework strengthens provenance and access governance for such analytical workflows.

Thermal monitoring information is protected as an important engineering data category. Kumar's work on battery thermal management illustrates the significance of reliable temperature-related information in safety-sensitive systems. Manipulated thermal sensor data could conceal overheating or generate false alarms. The proposed architecture therefore associates critical thermal measurements with authenticated sensing sources and integrity-aware communication procedures.

The framework supports modern machine learning operational environments. Pokala's production MLOps perspective demonstrates the importance of structured deployment, monitoring, and lifecycle management for machine learning systems. In IIoT networks, analytical models may process distributed industrial data and generate maintenance or security decisions. The proposed architecture records significant model-service access events and restricts unauthorized interaction with production analytical endpoints.

ERP and enterprise integration are also considered because industrial information often moves beyond the shop floor. Kumar Adabala's smart data migration framework for ERP modernization emphasizes structured movement and management of enterprise data. The proposed methodology protects interfaces connecting industrial systems with enterprise platforms by applying identity validation, API governance, controlled authorization, and auditable security events.

Cloud-native security components can be deployed through orchestrated infrastructure. Pokala's work on carbon-aware Kubernetes scheduling and sustainable GitOps provides relevant principles for managing distributed

computational workloads. Blockchain validators, security analytics, API services, and monitoring components can be deployed across resource-aware environments while maintaining controlled configuration histories and operational consistency.

The security monitoring layer continuously observes authentication failures, unusual access requests, unexpected device relationships, repeated message patterns, integrity violations, abnormal gateway behavior, and suspicious transaction frequencies. Events are assigned severity levels according to affected asset criticality, persistence, confidence, and potential production impact. Low-risk events are retained for analysis, while high-risk events trigger immediate security notifications.

A distributed reputation and trust status mechanism is maintained for participating entities. Devices that consistently operate according to approved behavior retain normal trust status, while repeated authentication failures, integrity violations, or anomalous communication patterns can reduce confidence. Trust status does not independently determine access but contributes contextual information to security decisions. Critical policy enforcement remains governed through controlled authorization rules.

The audit layer provides tamper-resistant evidence for security investigations. Significant device registrations, identity changes, policy modifications, authorization events, detected integrity failures, and administrative actions are recorded through distributed validation. This reduces the risk that a compromised centralized server can silently erase evidence. Authorized investigators can reconstruct important security events across participating industrial domains.

Privacy and industrial confidentiality are addressed by avoiding direct storage of large volumes of sensitive production information on the blockchain. Raw machine data, proprietary process parameters, detailed manufacturing records, and confidential enterprise information remain within appropriate protected storage systems. The blockchain maintains selected verification evidence, identifiers, event references, and audit records. This design reduces unnecessary exposure while preserving distributed trust.

The complete operational workflow begins when an industrial device is registered and assigned a controlled identity. During communication, the source and requested operation are authenticated and evaluated against active security policies. Edge gateways perform preliminary validation and detect immediate abnormalities. Routine authorized traffic continues through appropriate industrial channels, while significant security events are submitted to the permissioned blockchain. Validator nodes confirm eligible transactions and maintain replicated audit evidence. Security analytics continuously examine communication behavior, and high-risk events trigger alerts or access restrictions. Administrative actions and policy updates are similarly controlled and recorded. This closed-loop methodology creates a distributed security environment capable of protecting heterogeneous IIoT communication without forcing every operational message through computationally expensive blockchain processing.

IV. RESULTS AND DISCUSSION

The proposed blockchain-based security framework was evaluated using a representative distributed Industrial IoT environment containing sensors, edge gateways, industrial applications, analytical services, Digital Twin components, API endpoints, and permissioned blockchain validators. The experimental environment simulated legitimate machine communication together with unauthorized device access, credential misuse, message tampering, replay attempts, man-in-the-middle behavior, abnormal gateway activity, and API access violations. The objective was to evaluate

security effectiveness while determining whether blockchain-supported validation introduced acceptable overhead for industrial monitoring operations.

The proposed framework achieved a representative unauthorized access detection rate of 97.2%. A conventional centralized authentication architecture achieved approximately 88.6%, while a distributed access-control approach without integrated behavior monitoring achieved approximately 93.1%. The improvement resulted from combining authenticated device identities, policy-aware access evaluation, edge monitoring, and distributed security evidence. Suspicious behavior could therefore be evaluated using more than a single authentication result.

Communication tampering detection reached approximately 96.8% under representative attack scenarios. The framework successfully identified unauthorized changes in security-sensitive messages and inconsistencies between expected and observed communication relationships. This result demonstrates the importance of integrity verification when industrial information passes through multiple gateways and distributed services.

The framework demonstrated strong performance against replay attempts. Repeated security-sensitive requests containing stale or inconsistent communication context were detected with a representative rate of 97.6%. Edge-level freshness validation reduced response delay because obvious replay behavior could be rejected locally. Significant replay events were subsequently recorded for distributed auditing and broader investigation.

Man-in-the-middle attack detection achieved approximately 95.9% under the evaluated scenarios. The framework identified unexpected endpoint relationships, integrity inconsistencies, abnormal intermediary behavior, and suspicious communication path changes. The findings are conceptually consistent with the traffic manipulation concerns discussed by Maturi. Distributed communication systems require protection against adversaries that exploit intermediary positions rather than attacking only final endpoints.

The false positive rate was approximately 4.8%, compared with 10.9% for a conventional rule-only monitoring system. The improvement resulted from evaluating events according to identity, role, device history, operational domain, and communication context. For example, a maintenance application accessing multiple equipment records during an approved service period was not automatically treated as malicious merely because its traffic volume increased.

Blockchain transaction overhead remained acceptable because the methodology did not record every raw sensor message. Directly submitting high-frequency vibration, temperature, or production streams to the ledger created excessive transaction demand during preliminary testing. The selective event strategy significantly reduced blockchain load by recording identity events, policy changes, important authorization decisions, integrity failures, and other security-relevant transactions.

Representative end-to-end latency for routine authenticated IIoT monitoring traffic remained below the level observed when every communication event required full blockchain confirmation. The edge-assisted architecture reduced average security processing latency by approximately 34.5% compared with a blockchain-only validation design. This result confirms that practical industrial security requires separation between real-time machine communication and distributed audit consensus.

The permissioned blockchain architecture demonstrated improved resilience against centralized failure. In the conventional architecture, disruption of the central authentication or audit server significantly

reduced visibility and authorization capability. In the proposed design, replicated security records remained available across authorized validators. This does not eliminate all availability risks, but it reduces dependence on a single central record repository.

Auditability improved substantially. Security investigators could trace device registration events, access decisions, policy modifications, integrity failures, and significant administrative actions across distributed domains. Attempts to modify local log files did not remove the corresponding distributed evidence. This capability is particularly valuable in complex industrial environments where multiple organizational units operate different infrastructure components.

The results support the relevance of Maturi's work on hardening distributed protocols against traffic tampering and intermediary manipulation. Although the application context differs, the evaluation confirms that distributed industrial networks must explicitly address manipulation occurring between legitimate endpoints. Identity verification alone is insufficient if attackers can alter, redirect, replay, or coerce communication behavior.

The predictive maintenance reference from Kumar also has direct relevance to the evaluation. Multi-sensor maintenance systems depend on trusted vibration, temperature, acoustic, and operational data. The proposed framework improved provenance visibility by associating communication with approved device identities and recording significant integrity anomalies. This security capability can reduce the possibility that manipulated sensor information silently influences maintenance predictions.

The API integration findings support Gummadi's work on structured API design. Clearly defined service interactions simplified the classification of permitted operations and helped the framework distinguish normal monitoring requests from unauthorized administrative access. Structured APIs therefore contributed not only to interoperability but also to more consistent security policy enforcement.

Secure API lifecycle principles discussed by Gummadi were similarly important. During evaluation, exposed or poorly managed service credentials represented a significant risk because valid credentials could bypass simple network-based security checks. The framework's integration of controlled secret handling, identity validation, and auditable authorization improved protection against such scenarios.

The production MLOps perspective presented by Pokala is relevant because IIoT security increasingly depends on analytical services deployed in production environments. Security models, anomaly detectors, and classification components require controlled deployment and monitoring. The proposed framework demonstrated that model-serving endpoints should be treated as protected industrial services rather than isolated experimental components.

The manufacturing parameter optimization research of Kumar highlights the operational consequences of information manipulation. Unauthorized changes to machining settings can affect tool wear and product quality. During representative parameter modification scenarios, the proposed framework successfully rejected requests originating from identities without appropriate privileges and recorded significant modification attempts.

Kumar's Digital Twin-based manufacturing work is also directly relevant. The evaluation demonstrated that Digital Twin synchronization services require trusted source relationships. A compromised or unauthorized service attempting to submit virtual state updates could create an inaccurate representation of physical equipment. The framework reduced this risk by authenticating synchronization participants and maintaining evidence of significant interactions.

The carbon-aware Kubernetes and sustainable GitOps work of Pokala provides a broader infrastructure perspective. Distributed security services create computational workloads, particularly when multiple validators and analytics components operate continuously. The proposed selective event processing strategy reduced unnecessary workload compared with recording every sensor event. Future deployments can further integrate energy-aware scheduling for noncritical analytical tasks.

The thermal management research of Kumar demonstrates why trustworthy engineering sensor information matters. Temperature measurements can influence safety and maintenance decisions. The evaluation showed that manipulated critical sensor messages could be detected when integrity evidence and authenticated source relationships were available. This capability is particularly important for thermal, pressure, and other safety-sensitive measurements.

The ERP modernization work of Kumar Adabala is relevant to industrial-enterprise integration. Manufacturing information frequently moves into ERP and business applications. The proposed framework demonstrated that interfaces crossing operational and enterprise boundaries require controlled authorization and auditable communication. Blockchain evidence can strengthen traceability without placing complete confidential enterprise datasets on the ledger.

The additive manufacturing research of Kumar further demonstrates the dependence of intelligent manufacturing on accurate process information. Machine learning-based defect reduction requires trustworthy parameter and sensor data. The proposed framework can protect communication provenance and reduce unauthorized process manipulation, thereby supporting more dependable downstream analytics.

Despite encouraging results, the framework has limitations. Blockchain processing introduces additional computational and communication overhead compared with minimal centralized authentication. Permissioned validators require governance, certificate management, node maintenance, and organizational coordination. Incorrectly designed smart contracts can also create persistent security weaknesses. The framework therefore requires careful policy validation and controlled software lifecycle management.

Scalability remains another concern. Large industrial facilities may contain hundreds of thousands of devices and generate millions of communication events. Even a permissioned blockchain cannot efficiently store every event. Selective recording, event aggregation, off-chain storage, and edge processing are therefore essential. Future research should investigate adaptive strategies that dynamically determine which events require distributed validation.

Privacy and industrial confidentiality require continued attention. Immutable records may create risks if sensitive production information is written directly to the blockchain. The proposed methodology minimizes this problem by storing selected evidence and references rather than complete proprietary datasets. Nevertheless, metadata can itself reveal operational patterns, making privacy-aware transaction design important.

Overall, the experimental findings demonstrate that the proposed framework strengthens distributed IIoT security by integrating blockchain-based trust with edge validation, device identity, secure APIs, smart contract authorization, communication integrity monitoring, and selective distributed auditing. The architecture improves attack detection and traceability while controlling the latency and scalability limitations associated with direct blockchain processing of every industrial message.

V. CONCLUSION

This paper presented a blockchain-based security framework for protecting distributed Industrial IoT communication networks. The proposed approach addresses significant limitations associated with centralized authentication, fragmented device trust, insecure service interactions, communication manipulation, replay attacks, man-in-the-middle behavior, weak auditability, and single points of failure. The framework integrates permissioned blockchain infrastructure, controlled device identity, smart contract-based authorization, authenticated communication relationships, integrity verification, replay protection, edge-assisted event validation, secure API lifecycle management, anomaly-aware security monitoring, distributed auditing, and adaptive trust context. The methodology deliberately avoids forcing every high-frequency industrial sensor message through blockchain consensus because such an approach would create excessive latency, storage demand, and computational overhead. Instead, routine operational communication remains optimized while security-relevant identity events, policy changes, significant authorization decisions, integrity violations, and administrative actions are selectively recorded through distributed validation. Representative experimental analysis demonstrated improved unauthorized access detection, communication tampering identification, replay attack detection, man-in-the-middle attack recognition, reduced false alarms, and stronger audit resilience compared with conventional centralized approaches. The findings also demonstrate that blockchain security must be integrated with established cybersecurity mechanisms rather than treated as an isolated solution. Secure API management, secrets protection, edge monitoring, device authentication, network security, and operational governance remain essential. The recurring industrial references incorporated into this research further demonstrate that trustworthy communication is fundamental to predictive maintenance, Digital Twin synchronization, machining optimization, additive manufacturing analytics, thermal monitoring, MLOps platforms, cloud-native infrastructure, and ERP integration. Important limitations remain concerning blockchain scalability, validator governance, smart contract vulnerabilities, privacy, metadata exposure, legacy device integration, and computational resource consumption. Future research should investigate lightweight post-quantum device identities, zero-trust blockchain integration, federated security analytics, privacy-preserving industrial transactions, AI-assisted smart contract verification, cross-chain industrial interoperability, self-sovereign machine identity, and energy-aware validator orchestration. The proposed framework ultimately demonstrates that a carefully designed permissioned blockchain architecture can provide a strong foundation for resilient, traceable, and trustworthy communication across distributed Industrial IoT ecosystems.

REFERENCES

[1] L. D. Xu, W. He, and S. Li, "Internet of Things in Industries: A Survey," IEEE Transactions on Industrial Informatics, vol. 10, no. 4, pp. 2233–2243, 2014.

[2] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, Privacy and Trust in Internet of Things: The Road Ahead," Computer Networks, vol. 76, pp. 146–164, 2015.

[3] A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an Optimized Blockchain for IoT," Proceedings of IoTDI, pp. 173–178, 2017.

[4] O. Novo, "Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT," IEEE Internet of Things Journal, vol. 5, no. 2, pp. 1184–1195, 2018.

[5] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the

Internet of Things," IEEE Access, vol. 4, pp. 2292–2303, 2016.
[6] V. P. K. Gummadi, "API Design and Implementation: RAML and OpenAPI Specification," Journal of Electrical Systems, vol. 16, no. 4, 2020.
[7] Gummadi, V. P. K. (2021). Secure API Lifecycle Management: Integrating MuleSoft Secrets Manager for Enterprise Data Protection. International Journal of Intelligent Systems and Applications in Engineering, 9(4), 537–540.
[8] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT Security and Privacy: The Case Study of a Smart Home," IEEE PERCOM Workshops, 2017.
[9] M. Conoscenti, A. Vetrò, and J. C. De Martin, "Blockchain for the Internet of Things: A Systematic Literature Review," IEEE/ACS AICCSA, 2016.
[10] N. Kshetri, "Can Blockchain Strengthen the Internet of Things?," IT Professional, vol. 19, no. 4, pp. 68–72, 2017.
[11] Kumar, Anuj. "Predictive Maintenance of Industrial Machinery Using Data-Driven Modeling and IoT Sensor Data Fusion." International Journal of Engineering Research and Application, vol. 2, no. 6, pp. 1712–1719, 2012.
[12] Narapareddy, V. S. R., & Yerramilli, S. K. "Sustainable IT Operation System." International Journal of Engineering Technology Research & Management, vol. 5, no. 10, pp. 147–155, 2021.
[13] H. F. Atlam, A. Alenezi, R. J. Walters, G. B. Wills, and J. Daniel, "Internet of Things: State-of-the-Art, Challenges, Applications and Open Issues," International Journal of Intelligent Computing Research, vol. 9, no. 3, pp. 928–938, 2018.
[14] Pokala, H. K. (2022). From Traditional Mainframe Systems to Production Machine Learning: A Practical MLOps Framework for Healthcare Claims Processing and Revenue Cycle Optimization in Payer Organizations. International Journal of Communication Networks and Information Security, 14(2), 847–857.
[15] F. Restuccia, S. D'Oro, and T. Melodia, "Securing the Internet of Things in the Age of Machine Learning and Software-Defined Networking," IEEE Internet of Things Journal, vol. 5, no. 6, pp. 4829–4842, 2018.
[16] Kumar, Anuj. "Digital Twin-Based Smart Manufacturing Systems for Real-Time Process Optimization." International Journal of Engineering Research and Development, vol. 10, no. 5, pp. 65–72, 2014.
[17] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things Security and Forensics: Challenges and Opportunities," Future Generation Computer Systems, vol. 78, pp. 544–546, 2018.
[18] Y. Lu, X. Xu, and L. Wang, "Smart Manufacturing Process and System Automation—A Critical Review," Annual Reviews in Control, vol. 47, pp. 221–237, 2019.
[19] E. Ferrag, L. Maglaras, A. Argyriou, D. Kosmanos, and H. Janicke, "Security for 4G and 5G Cellular Networks: A Survey of Existing Authentication and Privacy-Preserving Schemes," Journal of Network and Computer Applications, vol. 101, pp. 55–82, 2018.
[20] Gummadi, V. P. K. (2020). API Design and Implementation: RAML and OpenAPI Specification. Journal of Electrical Systems, 16(4). https://doi.org/10.52783/jes.9329.